

**IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA**

UNITED STATES)	
)	
v.)	CR 18-292
)	
ROBERT BOWERS)	
)	

OPINION AND ORDER

SYNOPSIS

Defendant has filed a Motion to Suppress Evidence Seized During Search and Seizure from Internet Service Provider Information Associated with Target Accounts and Target IMEI (Motion to Suppress No. 7). [Docket Nos. 294 (Redacted Motion), 309 (Sealed Motion)]. The Government has responded [Docket Nos. 346 (Redacted Response), 363 (Sealed Response)]. Defendant has replied, and the Government has filed a Sur-reply. [Docket Nos. 380 (Redacted Reply), 391 (Sealed Reply), 401 (Sur-reply)]. For the following reasons, Defendant’s Motion will be denied in part, and the remainder held in abeyance pending argument and a hearing.¹

OPINION

Defendant contends that the Affidavit submitted in support of the warrant to search and seize information associated with two e-mail accounts and an International Mobile Equipment Identity Number (“IMEI”) failed to establish probable cause. The Google e-mail accounts at issue are ODGPhone@gmail.com and onedingo@gmail.com (“Target Accounts”); the IMEI number is 35527308f064040 (“Target IMEI”). In addition, Defendant contends that the warrant

¹ A hearing is required on a suppression motion if it raises issues of fact material to the resolution of the defendant's constitutional challenge. United States v. Hines, 628 F.3d 101, 105 (3d Cir. 2010). The defense bears the burden of demonstrating entitlement to a hearing. United States v. Stevenson, No. 16-189, 2019 U.S. Dist. LEXIS 172592, at *4 (W.D. Pa. Oct. 4, 2019). No hearing is required on the Motion at bar, except as indicated in the body of the Opinion.

relating to onedingo@gmail.com was overbroad, in that it failed to limit the information subject to seizure to those for which probable cause may have existed.

A. Target IMEI and Target Account ODGPhone@gmail.com

The Government argues that Defendant does not have standing to raise his challenge, as he has not demonstrated the requisite privacy interest in the Target Accounts and IMEI. For present purposes, I assume without deciding that Defendant has made the necessary showing as to the Target IMEI and the Target Account ODGPhone@gmail.com.²

A court does not conduct a de novo determination of probable cause, but instead determines whether a “substantial basis” existed for the magistrate’s finding. United States v. Carney, No. 06-350, 2007 U.S. Dist. LEXIS 46640, at *20 (W.D. Pa. June 27, 2007). The Court’s review rests on the affidavit of probable cause placed before the magistrate. United States v. Zimmerman, 277 F.3d 426, 431, n.3 (3d Cir. 2002). A reviewing Court is to “give great deference to the magistrate judge's probable cause determination.” Id. at 305. In addition, “[t]he resolution of doubtful or marginal cases in this area should be largely determined by the preference to be accorded to warrants.” United States v. Hodge, 246 F.3d301, 305 (2001).

The existence of probable cause is to be assessed through “a practical, common-sense decision whether, given all the circumstances set forth in the affidavit before [the magistrate], ...there is a fair probability that ... evidence of a crime will be found in a particular place.” Illinois v. Gates, 462 U.S. 213, 238, 103 S. Ct. 2317, 76 L.Ed.2d 527 (1983). In addition, the

² The proponent of a motion to suppress bears the burden of demonstrating that he had a legitimate expectation of privacy in the place to be searched; this inquiry “is shorthand for the determination of whether a litigant's Fourth Amendment rights have been implicated.” United States v. Stern, 597 F.3d 540, 551 (3d Cir. 2010) (quoting United States v. Mosley, 454 F.3d at 253 n. 5 (3d Cir. 2006)). Here, Defendant points to the facts set forth in the Affidavit and the Government’s assertions to make the requisite showing. The Government, as it does in connection with other Motions to Suppress, contends that Defendant cannot rely on its assertions to establish standing. When a Fourth Amendment challenge is subject to rejection on other grounds, courts routinely assume standing and reach the substantive challenge.

inquiry rests on the totality of the circumstances; each piece of information in an affidavit is not assessed in isolation. See Gates, 462 U.S. at 230-31. Accordingly, our Court of Appeals has cautioned against “‘overly compartmentaliz[ing]’ the determination of probable cause.” United States v. Yusuf, 461 F.3d 374, 390 (3d Cir. 2006). Instead, the Court must “consider the cumulative weight of the information set forth by the investigating officer in connection with reasonable inferences that the officer is permitted to make based upon the officer’s specialized training and experiences.” Id. In that vein, probable cause does not require direct evidence linking the place to be searched to the crime. Hodge, 246 F.3d at 305. In this context, “[a] court is entitled to draw reasonable inferences about where evidence is likely to be kept, based on the nature of the evidence and the type of offense. Id. at 305-06.

Moreover, “probable cause does not require that each factual allegation which the affiant puts forth must be independently documented.” Jaben v. United States, 381 U.S. 214, 224-25 (1965). Otherwise stated, each fact set forth does not have to be attributed to a particular source. United States v. Piquet, 372 F. App’x 42, 45 (11th Cir. 2010). Similarly, the police are “not required to track the details of how they become acquainted with widely known facts.”³ United States v. Berland, 1979 U.S. Dist. LEXIS 12983, at *29 (S.D.N.Y. Apr. 18, 1979). An attesting officer’s experience is relevant to the analysis. United States v. Castellanos, No. 15-2037, 2016 U.S. Dist. LEXIS 59743, at *11 (N.D. Iowa May 5, 2016).

These principles apply to “traditional” searches of physical space, and also in the context of the electronic realm: “For the requisite nexus to exist—regardless of whether the underlying crime requires the use of social media or an electronic device—the affidavit in support of the search warrant must establish why the government believes that relevant evidence may reside on

³ Defendant’s social media posts were widely reported in the national media in the days prior to October 30, 2018, the date appearing on the Affidavit. See, e.g., <https://www.theatlantic.com/technology/archive/2018/10/what-gab/574186/>; <https://apnews.com/article/b1c50ba4f0964df89a266e490aea6961> (accessed Feb. 12, 2021).

the particular suspect's [electronic] account." United States v. Whitt, 2018 U.S. Dist. LEXIS 7420, 2018 WL 447586, at *2 (S.D. Ohio, Jan. 17, 2018).⁴

In United States v. Tsarnaev, 53 F. Supp. 3d 450, 461-62 (D. Mass. 2014), the Court considered these principles as applied to a warrant to obtain a variety of information associated with e-mail accounts. In that case, the affidavit in support of the warrant stated that defendant had used one of the target e-mail accounts to apply for student aid, and that his deceased brother had provided the other target e-mail account to his college. Id. The affidavit further stated that “it appears” that both Defendant and his brother used social media; that defendant had a Facebook page; and that his brother had a YouTube page. Id. In addition, it averred that given defendant’s and his brother’s ages, their use of social media, and the fact that they provided e-mail addresses to the Department of Education and a Community College, “there is probable cause to believe that they used these e-mail accounts regularly, and that evidence of the crimes described in this affidavit would be found in them.” Id. The affidavit further stated as follows:

I also have probable cause to believe that the Subject Accounts and the data associated with those accounts contain evidence, fruits, and instrumentalities of the crimes identified above. I base this conclusion in part on my training and experience. I know that many people regularly use e-mail to provide contact information to others, as well as to discuss future plans and to make logistical arrangements. I also know, based on my training and experience, that many criminals use e-mail to plan and discuss their criminal schemes.

Id. at 462.

The Court determined that there was no reason to conclude that the magistrate could not have accepted the suggested inference, and made a “‘practical, common-sense decision’ that

⁴ In terms of obtaining account records from a third-party provider, another court has observed: “[E]very case of which we are aware that has entertained a suppression motion relating to the search of an email account has upheld the Government’s ability to obtain the entire contents of the email account to determine which particular emails come within the search warrant.” United States v. USPlabs, LLC, No. 3:15-CR-496-L, 2019 U.S. Dist. LEXIS 29238, at *44 (N.D. Tex. Feb. 24, 2019) (quoting In the Matter of a Warrant for All Content & Other Info. Associated with the Email Account xxxxxxxx gmail.com Maintained at Premises Controlled By Google, Inc., 33 F. Supp. 3d 386, 394 (S.D.N.Y. 2014), as amended (Aug. 7, 2014)).

there was a ‘fair probability’ that, because it was likely the defendant actively used his...email account, some evidence of the criminal activity referred to in the affidavit could be expected to be found in the...email accounts.” Id. at 462-63.

In this case, the Affidavit and subsequent warrant related to information for the subject Target Account and IMEI for the time period from August 27, 2018 to October 27, 2018. [Docket No. 309, Ex. 1, p. 4].⁵ The Affidavit was sworn and subscribed on October 30, 2018. Id. at p. 21. It set forth the events of October 27, 2018 at the Tree of Life synagogue. Id. at p. 9, ¶8. It stated that during the attack, Defendant made audible statements regarding genocide, his desire to kill Jewish people, and that Jewish people needed to die. Id. at p. 4, ¶12. It further stated that “[f]rom on or about September 18, 2018, [Defendant] has made numerous anti-Semitic statements on internet posts, indicating that [Defendant] had access to the internet and/or internet capable devices.” Id. at ¶13. It states that Defendant has at least 14 weapons registered in his name. Id. at p. 10, ¶16. In addition, the Affidavit states that “[e]arly indications through the investigation are that [Defendant] engaged in planning and premeditation prior to executing the killings and injury associated with this crime.” Id. at ¶21.

The Affiant identified his employment as a special agent with the FBI since 2007, his work on investigations including violent crime and criminal cyber investigations, and his training, including computer crime investigations and the identification and collection of computer-related evidence. Id. at p. 8, ¶3. He stated that his belief in probable cause was based on the facts set forth in the Affidavit, as well as his “training and experience.” Id. at ¶5. Following a lengthy description of the types of data that might be obtained from Google, the Affiant states:

⁵ Page numbers used herein refer to the as-docketed page numbers, rather than those page numbers internal to each document.

In my training and experience, evidence of who was using a Google account, and from where, and evidence related to criminal activity of the kind described below, may be found in the files and records above....Based on my training and experience, instant messages, emails, voicemails, photos, videos, and documents are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation.

Id. at p. 18, ¶29.

He further noted that account-related evidence could provide insight into the account owner's state of mind as it relates to the offenses under investigation, or the identities of co-conspirators and instrumentalities of the crimes under investigation. Id. at p. 31, ¶¶31-32.

In terms of the targets of the search at issue, FBI agents determined that the T-Mobile device with the Target IMEI belonged to Defendant; historical cell site data responsive to a separate warrant included the Target IMEI.⁶ Id. at p. 5, ¶23. One of Defendant's family members provided agents with the name of the subject Target Account and identified it as "often utilized" by Defendant. Id. at ¶¶23-25. The family member further advised agents that the Target Account was linked to Defendant's cellular telephone, and that he used it when on the road without access to his laptop. Id. at ¶24. The Affidavit identified the items to be seized as "[a]ll information described above that constitutes evidence of violations of" 18 U.S.C. §§ 247(a)(2) and (d)(1), 924©(1)(A) and (j)(1), 247(a)(2) and (d)(3), at 924(c)(1)(A)(iii). Id. at p. 5.

In light of applicable standards, the cumulative weight of the information in the Affidavit provided a substantial basis for Magistrate Judge Mitchell's probable cause finding as to Target Account ODGPhone@gmail.com and the Target IMEI. As in Tsarnaev, there is no reason that Magistrate Mitchell could not have accepted the inference that Defendant used the Target Account and cell phone connected with the Target IMEI, and concluded that there was a fair probability that they would contain evidence of the identified criminal activity. The fact that the

⁶ Historical cell site data is addressed in connection with Defendant's Motion to Suppress No. 6.

Affidavit does not explicitly, independently source each fact does not negate the reasonable inferences to be drawn from the totality of the information in the Affidavit. The same is true for the purported lack of explicit, direct connections between the use of the Target Account or Target IMEI and a criminal act. There is no suggestion that agents relied on a confidential informant or anonymous tip; instead, the pertinent stated sources of information are the investigation, which included an interview with a member of Defendant's family, and the Affiant's experience and training. Defendant's motion will be denied as to the Target IMEI and Target Account ODGPhone@gmail.com.

In the alternative, even if probable cause had been lacking as to the Target IMEI and Target Account ODGPhone@gmail.com, the good faith exception to the exclusionary rule would apply. The goal of the exclusionary rule is to deter Fourth Amendment violations. See, e.g., United States v. Caesar, No. 19-3961, 2021 U.S. App. LEXIS 18692, at **15-17 (3d Cir. June 23, 2021); United States v. Werdene, 883 F.3d 204, 215 (3d Cir. 2018). If officers acted with an "objectively reasonable good-faith belief that their conduct [was] lawful," deterrence is not a justification for exclusion of evidence. United States v. Katzin, 769 F. 3d 163, 171 (3d Cir. 2013). The good faith inquiry rests on "the objectively ascertainable question whether a reasonably well trained officer would have known that the search was illegal' in light of 'all of the circumstances.'" United States v. Horton, 863 F.3d 1041, 1051 (8th Cir. 2017) (quoting Herring v. United States, 555 U.S. 135, 145, 129 S. Ct. 695, 172 L. Ed. 496 (2009)). Given the social cost of suppressing evidence, the Supreme Court has described the remedy as a "last resort" rather than a "first impulse." Hudson v. Michigan, 547 U.S. 586, 591, 126 S. Ct. 2159, 2163, 165 L.Ed. 2d 56 (2006). Had this Court determined that the warrant was illegal, the

discussion supra makes clear that they were not so facially deficient, or so lacking in indicia of probable cause, as to warrant suppression of the evidence.

B. Target Account onedingo@gmail.com

In addition to raising the challenges addressed supra, Defendant also contends that the warrant was overbroad, to the extent that it authorized the search and seizure of records from Target Account onedingo@gmail from December, 2007 to March, 2008. The Court will hold Defendant's challenges concerning Target Account onedingo@gmail.com in abeyance pending argument.

CONCLUSION

In conclusion, Defendant's Motion to Suppress No. 7 will be denied in part, and the remainder held in abeyance. The totality of the affidavit, and reasonable inferences to be drawn from the averments therein, provided the requisite basis for the Magistrate Judge's probable cause determination as to Target Account ODGPhone@gmail.com and the Target IMEI. The portion of the Motion relating to Target Account onedingo@gmail.com will be held in abeyance pending argument. An appropriate Order follows.

BY THE COURT:



Donetta W. Ambrose
Senior Judge, U.S. District Court

Dated: July 8, 2021

**IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA**

UNITED STATES)	
)	
v.)	CR 18-292
)	
ROBERT BOWERS)	
)	

ORDER

AND NOW, this 8th day of July, 2021, it is hereby ORDERED, ADJUDGED, and DECREED that Defendant's Motion to Suppress Evidence Seized During Search and Seizure from Internet Service Provider Information Associated with Target Accounts and Target IMEI (Motion to Suppress No. 7). [294 (Redacted Motion), 309 (Sealed Motion)] is DENIED in part. The Motion is denied as to Target Account ODGPhone@gmail.com and the Target IMEI. As to Target Account onedingo@gmail.com, the Motion is held in abeyance pending argument. A hearing shall be scheduled by separate Order of Court.

BY THE COURT:



Donetta W. Ambrose
Senior Judge, U.S. District Court